The Bitcoin mining games

Nicolas Houy

GROUPE D'ANALYSE ET DE THÉORIE ÉCONOMIQUE LYON - ST ÉTIENNE

WP 1412

The Bitcoin mining game

Nicolas Houy

March 2014

GATE Groupe d'Analyse et de Théorie Économique Lyon-St Étienne

93, chemin des Mouilles 69130 Ecully – France
Tel. +33 (0)4 72 86 60 60
Fax +33 (0)4 72 86 60 90

6, rue Basse des Rives 42023 Saint-Etienne cedex 02 – France
Tel. +33 (0)4 77 42 19 60
Fax. +33 (0)4 77 42 19 50

Messagerie électronique / Email : gate@gate.cnrs.fr
Téléchargement / Download : http://www.gate.cnrs.fr – Publications / Working Papers

The Bitcoin mining game

v.0.1

Nicolas HOUY*

March 11, 2014

Abstract

When processing transactions in a block, a miner increases his reward but also decreases his probability to earn any reward because the time needed for his block to reach consensus depends on its size. We show that this leads to a game situation between miners. We analytically solve this game for two miners. Then, we show that miners do not play a Nash equilibrium in the current Bitcoin mining environment, instead, they should not process any transaction. Finally, we show that the situation where no transaction is ever processed would stop being a Nash equilibrium if the transaction fee was multiplied or, equivalently, the fixed reward divided by a factor of about 12.

JEL Classification: C72, D62.
Keywords: Bitcoin, mining, crypto-currency, game.

1 Introduction

Bitcoin[1] has been invented in 2008 ([Nakamoto, 2008]) but it really became popular and left the circle of strict early adopters in 2013. At the time this article is written, bitcoins can be bought and sold at about $620 apiece on some exchange markets. The monetary base is about $7,700,000,000. Bitcoin is usually described by laymen as an electronic or internet money even though this definition is much criticized by the computer science community that rather talks about a disruptive and revolutionary protocol. As a protocol, Bitcoin is still in its early stages of development and its specifications are still often modified. In order to reach the stage of implementation, a proposed modification goes through a whole process of validation. Some questions regarding some specifications of the Bitcoin protocol are still more or less open, transitory or left undecided. Among those questions is the value and structure of the rewards earned by the *miners*. In this paper, we analyze this aspect

*Université de Lyon, Lyon, F-69007, France; CNRS, GATE Lyon Saint-Etienne, Ecully, F-69130, France. E-mail: houy@gate.cnrs.fr.

[1]As the norm tends to be, we will write "Bitcoin" for the network or the protocol and "bitcoin" (or BTC) for each of the tokens that circulate on it.

of the Bitcoin protocol. Notice that the study we lead in this article are inspired by the qualitative intuitions given in [Andresen, 2013].

In order to do that, we need to describe, even superficially, how Bitcoin actually works. When an individual sends some bitcoins to another individual, this information is broadcast to the peer-to-peer Bitcoin network. However, for technical purposes we won't address here, this transaction needs to be included, together with other transactions forming a *block*, in the *blockchain* in order to be confirmed and secured. The blockchain is a public ledger that contains the full history of all the transactions in bitcoin ever processed. It is the role of miners to do this work of confirming and securing[2] transactions. Practically, this mining process consists in solving a mathematical problem and spreading the result to the Bitcoin network for it to reach consensus.[3] The first miner to do so sees his block included in the blockchain. As it requires computational resources, the successful miner is rewarded in bitcoins for his useful work. In the current implementation of Bitcoin, this reward comes from both an *ex-nihilo* creation of some new bitcoins and some fees Bitcoin users can add to their transactions. In order to control the monetary base, mining is made more complex than it could be. And since, in the first approximation, the probability for each miner to solve a mining problem depends on his computational power, the complexity of mining is made dependent on the total computational power of all miners. Precisely, the complexity is dynamically adjusted so that a block solving and hence a creation of bitcoins occurs every ten minutes in expectation.

In this article, we tackle the question of the incentives the miners face as a function of the reward structure and values. First, let us see the possible gains. As it is today, the fixed reward is 25 BTC per block. The fixed reward was 50 BTC in the first days of Bitcoin and this amount is halved every 210,000 blocks. Hence, the number of bitcoins issued is programmed to asymptotically reach a maximum of 21,000,000. At the time this article is written, there are about 12,500,000 bitcoins in circulation. The variable reward is 0.0001 BTC per transaction.[4] Second let us see the cost structure. When mining a block, a miner is free to choose which of the transactions in the network he wishes to include in his block. In a very good first approximation, computing the mining mathematical problem with more transactions included in it is not more expensive in terms of CPU, disk or bandwidth. However, it should be considered that the larger a block, the longer it takes for it to be spread in the Bitcoin network and reach consensus. Then, including transactions in a block can have the adverse effect of lowering the probability of a miner to earn any reward. When a block is mined but is outraced by another, it becomes *orphaned*.

[2]This security aspect of the mining activity is often forgotten or not know by the Bitcoin critics, see [Krugman, 2013] for instance. Even though their name can lead to confusion, Bitcoin miners have very little in common with gold miners and their role is very different in the Bitcoin protocol.

[3]We will say with no difference "solving" a mathematical problem" and "solving" or "finding a block".

[4]In reality, transactions can have different sizes in bytes and require different levels of fees to be computed. The size of a transaction depends on many parameters (number of inputs and outputs mainly) but not directly on the amount paid in the transaction. Throughout this article, we will make the simplifying assumption that all transactions have same size. At the time this article is written, the transaction fees represent about 0.4% of the miners' rewards. The remaining 99.6% are newly created bitcoins.

As we will show, this trade-off depends on how many transactions other miners include in their blocks themselves. Then, the number of transactions included in blocks is the outcome of a game: the Bitcoin mining game that we propose to study in this article.

In Section 2, we describe the Bitcoin mining game. In Section 3, we analytically study the equilibria of this game in the case with two miners. In Section 4, we study the current situation of the Bitcoin mining environment. We show that Bitcoin miners are not at a Nash equilibrium and a unilateral deviation could increase its author's benefit up to 2%. We also show that with the current incentives, miners should simply all play the strategy of including no transaction in their blocks. Finally, we will show that, if the miners' relative computational power distribution remains the same, the equilibrium where no miner includes a transaction in a block will stop being one in about 15 years or today if the transaction fee is increased by a factor 12.

2 Model

Let us consider a set $N = \{1, ..., N\}$ of miners on the Bitcoin network with $N \geq 2$.[5] Each miner $i \in N$ has a relative hash power $\alpha_i > 0$ such that $\sum_{j \in N} \alpha_j = 1$. Miners struggle against each other in a race to find the solution of a mathematical problem. This mathematical problem is solved by a try and guess strategy such that the occurrence of solving the problem can be modeled as a random variable following a Poisson process. The complexity of finding a block is dynamically adjusted so that this operation takes 600 seconds in expectation. Then, the mining Poisson process of the mining process has a parameter $\lambda = 1/600 > 0$ for the whole network.

The number of transactions included in a block to be solved is chosen by each miner. This number has no effect on the complexity of the mathematical problem or on the cost to solve it. However, once a miner has found a block with a given number of transactions in it, he needs to broadcast his solution to the Bitcoin network and his solution must reach consensus. Now, the time needed for a block to reach consensus is depending on the number of transactions included in this block. Let $k(x)$ be the time needed for a block including x transactions to reach consensus. We will make the assumption that this time function is linear, $k(x) = k.x$ with $k > 0$. The first miner to have found a block that reaches consensus earns (in bitcoins) a fixed reward $R \geq 0$ and a variable one $c.x$ with $c \geq 0$.

We assume that all miners start trying to find a new block at the same time. Each miner $i \in N$ includes $x_i > 0$ transactions in the block he tries to find. Let $\overrightarrow{x} = (x_1, ..., x_n)$ be the sequence of the numbers of transactions included in the new block to be found, one for each miner. Obviously, the probability for i to find a block between t and $t + dt$ and

[5] With a slight of rigor but with no risk of confusion, N denotes both the set of miners and the cardinality of this set.

that this block will be the first to reach consensus is

$$\left[\prod_{j\in N, t+k(x_i)-k(x_j)\geq 0} \exp(-\lambda\alpha_j(t+k(x_i)-k(x_j)))\right]\lambda\alpha_i dt. \quad (1)$$

After simple calculation, for any miner $i \in N$, the probability $P_i(\overrightarrow{x})$ to find a block and that this block will be the first to reach consensus is

$$P_i(\overrightarrow{x}) = \alpha_i\lambda\int_{t=0}^{\infty}\exp\left(-\lambda\left((1-Q_i(\overrightarrow{x},t))(t+k(x_i))+A_i(\overrightarrow{x},t)-\overline{k}\right)\right)dt, \quad (2)$$

where

$$\overline{k} = \sum_{j\in N}\alpha_j k(x_j),$$

and $\forall i \in N, \forall t > 0$,[6]

$$Q_i(\overrightarrow{x},t) = \sum_{j\in N}\alpha_j \mathbf{1}_{(k(x_j)>t+k(x_i))},$$

$$A_i(\overrightarrow{x},t) = \sum_{j\in N}\alpha_j k(x_j)\mathbf{1}_{(k(x_j)>t+k(x_i))}.$$

The expected reward $\Pi_i(\overrightarrow{x})$ is equal to the probability to find the first block to reach consensus times the reward if this is the case.

$$\Pi_i(\overrightarrow{x}) = (R+c.x_i)P_i(\overrightarrow{x}). \quad (3)$$

The following is straightforward from Equations 1 and 3.

Proposition 1

Let $i \in N$.

1. $\forall j \in N\setminus\{i\}, \dfrac{\partial\Pi_i(\overrightarrow{x})}{\partial x_j} \geq 0$,
2. $\forall j \in N\setminus\{i\}, \dfrac{\partial\Pi_i(\overrightarrow{x})}{\partial x_j} > 0$ *whenever* $(R+c.x_i) > 0$,
3. $\dfrac{\partial\Pi_i(\overrightarrow{x})}{\partial x_i} < 0$ *whenever* $c = 0$ *and* $R > 0$,
4. $\dfrac{\partial\Pi_i(\overrightarrow{x})}{\partial x_i} = 0$ *whenever* $c = 0$ *and* $R = 0$.

[6] For any proposition p, the indicator function $\mathbf{1}_p$ is equal to 1 if p is true, 0 otherwise.

Proposition 1 shows that introducing transactions in blocks by a miner has positive externalities on other miners (and hence that our game theoretical approach is justified). Indeed, when a miner $i \in N$ introduces more transactions in his block, he makes longer the time needed to spread his block, in turn allowing more time for other miners to find the next block, spread it to the network and reach consensus with it. However, this does not imply that the expected reward decreases for i. Indeed, it is true that introducing more transactions in the block he is looking for decreases i's probability to find and spread it first. But it also increases the reward he earns in case he is actually the first one to find and spread the next block. Of course, for this reasoning to be valid, we need to have $c > 0$ or else the marginal benefit to include transactions in blocks vanishes. In the trivial case where $c = 0$ and $R = 0$, the benefits of mining is obviously 0 anyway: there is nothing to earn whatever the sequence $\overrightarrow{x}$.

Generally, in order to decide the optimal number of transactions to include in a block, each miner $i \in N$ solves the following maximization program.

$$\max_{x_i \in \mathbb{R}^+} \Pi_i(\overrightarrow{x}). \tag{4}$$

We will need the following Lemma in the remainder. Assume that all miners include the same number of transactions in their blocks, formally, $\forall i \in N, x_i = x$. Then, for each miner $i \in N$, the probability to earn the reward associated with a block solving is just the probability to solve the mining mathematical problem first and hence is directly proportional to the hash rate α_i. Formally, in this case, $\forall i \in N, \forall t \geq 0, A_i(\overrightarrow{x}, t) = Q_i(\overrightarrow{x}, t) = 0$ and Lemma 1 is proved with simple calculation.

Lemma 1

If $\forall i \in N, x_i = x$, *then* $P_i(\overrightarrow{x}) = \alpha_i$ *and* $\Pi_i(\overrightarrow{x}) = (R + cx)\alpha_i$.

For the sake of simplicity, we will now concentrate on the case with $N = 2$ even though most of our results can be generalized to the $N > 2$ case with no logical difficulty but at the price of cumbersome calculation.

3 The two miners case

Let $N = \{1, 2\}$. For any miner $i \in N$, if $x_i \geq x_{3-i}$,[7] then $\forall t > 0$, $Q_i((x_1, x_2), t) = 0$ and $A_i((x_1, x_2), t) = 0$. Then, the expected reward earned by miner i is

$$\Pi_i(x_1, x_2) = \Pi^+(x_i, x_{3-i}) = (R + c.x_i)\alpha_i \exp\left(-(1 - \alpha_i)\lambda(k(x_i) - k(x_{3-i}))\right).$$

Following, assume $x_i < x_{-i}$, the expected reward earned by miner i is

$$\Pi_i(x_1, x_2) = \Pi^-(x_i, x_{3-i}) = (R + c.x_i)\left(1 - (1 - \alpha_i)\exp\left(-\alpha_i\lambda(k(x_{3-i}) - k(x_i))\right)\right).$$

[7] Obviously, if $i = 1$, $3 - i = 2$ and if $i = 2$, $3 - i = 1$.

Let $NE \subseteq 2^{(\mathbb{R}^+)^2}$ be the set of Nash equilibria of the mining game. Formally, $\forall (x_1^*, x_2^*) \in (\mathbb{R}^+)^2$, $(x_1^*, x_2^*) \in NE$ if and only if $x_1^* \in \arg\max_{x_1 \in \mathbb{R}^+} \Pi_1(x_1, x_2^*)$ and $x_2^* \in \arg\max_{x_2 \in \mathbb{R}^+} \Pi_2(x_1^*, x_2)$.

Our first result is rather trivial and follows directly from Proposition 1(3). When $c = 0$ and $R > 0$,[8] including a transaction in a block has the only consequence to make longer the period needed for a miner's block to reach consensus. The marginal reward associated with this inclusion is null. Hence, there are only negative incentives for miners to include transactions in blocks.

Proposition 2

Let $c = 0$ and $R > 0$. The Bitcoin mining game has a unique Nash equilibrium $(x_1^*, x_2^*) \in (\mathbb{R}^+)^2$ with $x_1^* = x_2^* = 0$. Moreover, $\Pi_1(x_1^*, x_2^*) = \alpha_1 R$ and $\Pi_1(x_1^*, x_2^*) = \alpha_2 R$.

For non trivial cases with $c > 0$, let us first concentrate on the symmetric games, i.e. on the cases with equal hash power, $\alpha_1 = \alpha_2 = 1/2$. For each of these games, there exists a unique Nash Equilibrium and it is symmetric.

Proposition 3

Let $c > 0$. Assume $\alpha_1 = \alpha_2 = 1/2$. The Bitcoin mining game has a unique Nash equilibrium $(x_1^*, x_2^*) \in (\mathbb{R}^+)^2$ with $x_1^* = x_2^* = \max\left\{0, \frac{2}{\lambda k} - \frac{R}{c}\right\}$. Moreover, $\Pi_1(x_1^*, x_2^*) = \Pi_2(x_1^*, x_2^*) = \max\left\{R/2, \frac{c}{\lambda k}\right\}$.

Then, in the symmetric case, Nash equilibria are symmetric. This is in line with the idea that when including transactions in blocks, a miner has a positive externality on other miners. Indeed, if there was a difference between two identical miners, say $x_1 < x_2$, 1 would marginally benefit more from 2's action than 2 would benefit from 1's action. Hence there exist a force for 1 to increase the number of transactions to include in his block and a force for 2 to decrease the number of transactions to include in his block. Then, a trend toward equalization of actions. Notice also that the fact that including transactions in blocks has positive externalities implies a globally low level of transactions included in blocks. Indeed, if the two miners were cooperating and maximizing the sum of the profits, they would choose x_1 and x_2 as large as possible.

Now, let us study the asymmetric case. With no loss of generality, let us assume $\alpha_1 > \alpha_2$.

Proposition 4

Let $c > 0$. Assume with no loss of generality, $\alpha_1 > \alpha_2$. The Bitcoin mining game has a unique Nash equilibrium $(x_1^*, x_2^*) \in (\mathbb{R}^+)^2$ with

- *if $\frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c} \leq 0$, $x_1^* = x_2^* = 0$.*

[8] Obviously, when both $c = 0$ and $R = 0$, the result is even more trivial since all miners' payoff are 0 whatever their and others miners' actions (Proposition 1(4)).

- *if* $\frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c} > 0$, $x_1^* = \frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c} > x_2^* \geq 0$.

In the asymmetric case, there is still a large set of parameters for which not including any transaction in a block for both miners is the only Nash equilibrium of the Bitcoin mining game. We can also notice that the number of transactions included by the miner with the greatest hash power is larger than the number of transactions included by the miner with the lowest hash power.

Obviously, as one of the main interests of Bitcoin is to serve as a payment system, it is of great importance to check for the plausibility of the set of parameters for which miners do not include transactions for processing in their blocks. If it were the case, Bitcoin could definitely not be used as a payment system. This is the motivation to study the mining environment as it is today.

4 The current case

In this Section, we study the current behavior of the actual miners in the Bitcoin network. Concretely, miners are rather mining pools but we will make no difference as we consider that the best strategy for a mining pool is the same whether it is a pool or a single miner, benefits being redistributed among the participants of the pool. All the data we need for this study is made public in the Bitcoin blockchain and protocol[9] or relies on the assumption based on personal expertise and experience that, today, all miners include all the transactions in the network when trying to find a block. Unless otherwise stated, the values for our computations are displayed in Table 1. We will also consider that the Bitcoin network hash power is distributed as shown in Table 2 (row B). We inferred these relative hash powers of miners from an analysis of the blocks found. Indeed, if we make, as already noted, the assumption that all miners include all the transactions in the network in their blocks, then, by Lemma 1, the probability to solve a block for any miner is exactly equal to his relative hash power. Further, we make the assumption that the frequency of blocks found by a miner[10], that we can observe, is the probability that he solves a block and, hence, his relative hash power.

Let us start our analysis of the current situation displayed in Table 2. We make the assumption that there are 320 transactions in the network. This is the average number of transactions in the blocks inserted in the blockchain in the year preceding our study (and this number is rather stable). As we said above, it is today's practice that when mining a block, all miners introduce all 320 transactions in the block they are mining. Formally, $\forall i \in N, x_i = 320$. In this case, by Lemma 1, the probability to find a block first (and equivalently to be the first to see his block reach consensus), is equal to its share of the total hash power (row B). We can now consider each miner and compute his best response

[9] The data we use from the blockchain are based on last-year averages as recorded on March 5$^{\text{th}}$, 2013. Data from the protocol can be found in the Bitcoin open-source code.

[10] The data we use from the blockchain for the block solving frequency are based on 3 last days averages as recorded on March 5$^{\text{th}}$, 2013.

Data	Value	Dimension	Description and Source
λ	1/600	second^{-1}	Bitcoin protocol parameter.
s	0.5	kB	Average transaction size, statistics from the blockchain.
k_b	0.08	second.kB^{-1}	Marginal time needed to reach consensus per kB, [Decker and Wattenhofer, 2013].
k	0.04	second.tx^{-1}	Marginal time needed to reach consensus per transaction (tx), $k_b.s$.
c	10^{-4}	BTC	Bitcoin protocol current implementation parameter.
R	25	BTC	Bitcoin protocol current implementation parameter.

Table 1: Data values.

to the other miners' current strategy. This optimal number of transactions to include in the current computed block is 0 for all miners (row D). This shows that the current situation is not a Nash Equilibrium. Stronger, all miners have a profitable deviation. If unilaterally mining blocks with no transaction, a miner would increase his probability to earn the fixed 25 BTC reward (row E) at the cost of the $320 \times 0.0001 = 0.32$ BTC variable reward in case of successful mining. In the current case, this deviation would lead to a higher expected benefit (rows F,G).

We can also check that all miners including no transaction in the block they are mining ($\forall i \in N, x_i = 0$) is a Nash Equilibrium with the current parameters given in Table 1. The expected reward for miner i, in this case where $\forall j \in N, x_j = 0$ is $\alpha_i.R$ by Lemma 1. The actual values are given in Table 3.

Now, we study the conditions under which the situation where all miners include no transaction in their blocks is a Nash equilibrium. Said differently, when no miner should include any transaction in their blocks, Bitcoin fails at being an efficient payment system. Hence, we look at the set of parameters for which a minimum requirement for Bitcoin to be a usable payment system is met. From Equation 3, it is straightforward to see that $\Pi_i(\overrightarrow{x}) = (R + cx_i)\alpha_i \exp\left(-\lambda(1-\alpha_i)k(x_i)\right)$ whenever $\overrightarrow{x}$ is such that $\forall j \in N \setminus \{i\}, x_j = 0$. Then, since $c > 0$, the best response number of transactions to include in a block by $i \in N$ is[11] $\arg\max_{x_i>0} \Pi_i(\overrightarrow{x}) = \{\max\{0, \frac{1}{\lambda(1-\alpha_i)k} - \frac{R}{c}\}\}$. Then, the situation where all miners include no transaction in their blocks stops being a Nash equilibrium when $\exists i \in N, \frac{c}{\lambda(1-\alpha_i)k} > R$. The highest value of R for which this occurs is $R \approx 2.03$ BTC below which GHash.IO will have an incentive to include some transactions in the block it tries to mine. Since R halves about every 4 years, this situation will occur in about 15 years with

[11] The proof is similar to the proof of Lemma 5 given in Appendix and is therefore omitted.

A	B	C	D	E	F	G
GHash.IO	26.012%	6.51121	0	26.421%	6.60525	1.444%
BTCGuild	22.736%	5.69128	0	23.110%	5.77747	1.514%
Eligius	19.075%	4.77489	0	19.404%	4.85095	1.593%
DiscusFish	11.946%	2.99034	0	12.170%	3.04254	1.746%
Deepbit	9.056%	2.26687	0	9.231%	2.30785	1.808%
BitMinter	3.276%	0.81993	0	3.343%	0.83577	1.932%
Slush	3.083%	0.77170	0	3.147%	0.78664	1.936%
Bitparking	0.963%	0.24116	0	0.984%	0.24594	1.982%
BTCMine	0.963%	0.24116	0	0.984%	0.24594	1.982%
50BTC	0.963%	0.24116	0	0.984%	0.24594	1.982%
OzCoin	0.771%	0.19292	0	0.787%	0.19676	1.986%
Polmine	0.385%	0.09646	0	0.394%	0.09839	1.994%
P2Pool	0.385%	0.09646	0	0.394%	0.09839	1.994%
EclipseMC	0.193%	0.04823	0	0.197%	0.04920	1.999%
ASICMiner	0.193%	0.04823	0	0.197%	0.04920	1.999%

Table 2: A: miner's name, B: relative hash power, C: expected reward when $\forall i \in N, x_i = 320$, D: optimal number of transaction included by miner i in the current block when $\forall j \in N \setminus \{i\}, x_j = 320$, E: probability to be the first miner to find a block reaching consensus when $\forall j \in N \setminus \{i\}, x_j = 320$ and x_i given in D, F: expected reward when $\forall j \in N \setminus \{i\}, x_j = 320$ and x_i given in D, G: (F-C) in %.

$R = 1.5625$.[12] In this case, the best response of GHash.IO will be to include 4,648 (or any smaller upper limit if it exists) transactions in a block. The other miners' best responses for $R = 1.5625$ are given in Table 4.

Equivalently, the lowest value of c for which the situation where all miners include no transaction in their blocks is not a Nash equilibrium is $c \approx 0.00123$ BTC. Above this value, GHash.IO will have an incentive to include some transactions in the block it tries to mine. This corresponds to an increase from the current value of the transaction fee of a factor approx. 12.3. At the time this article is written, 0.00123 BTC can be bought for about \$0.76.

5 Conclusion

In this article, we have introduced and studied the Bitcoin mining game. When miners make a decision regarding how many transactions they should include in the block they are

[12] Obviously, this 15 years projection should be seen as an illustration rather than a prediction. Indeed, it would certainly be unsound to state that in 15 years the mining environment will be unchanged, especially regarding the hash rate distribution among miners and k that highly depends on bandwidth (see the Nielsen's Law of Internet Bandwidth).

Mining pool	Expected reward
GHash.IO	6.50289
BTCGuild	5.68401
Eligius	4.76879
DiscusFish	2.98651
Deepbit	2.26397
BitMinter	0.81888
Slush	0.77071
Bitparking	0.24085
BTCMine	0.24085
50BTC	0.24085
OzCoin	0.19268
Polmine	0.09634
P2Pool	0.09634
EclipseMC	0.04817
ASICMiner	0.04817

Table 3: Expected reward of miners in BTC when $\forall i \in N, x_i = 0$.

mining, they must study the trade-off between, on the one side, including more transactions and hence earn more transaction fees if they find the current block first and, on the other side, including less transactions in order to minimize the time they need to spread their block solution and reach consensus with it, hence maximizing their probability to include their block in the blockchain first. We have studied the two miners case analytically. We have also showed that in the current Bitcoin mining environment, miners are not at a Nash equilibrium of the Bitcoin mining game. Instead, they should all stop including any transaction in their blocks. Finally, we showed that this situation where all miners do not include any transaction in their blocks would stop being a Nash Equilibrium if the transaction fee was multiplied or, equivalently, the fixed reward divided by a factor of about 12.

We can see two limitations to our study. The first one is about the security of the Bitcoin system. As we said, for Bitcoin to be used as an efficient payment system, it is a minimal requirement that transactions be processed. However, this is not sufficient. Indeed, Bitcoin is vulnerable to what is called 51% attacks (see [Eyal and Sirer, 2013, Kroll *et al.*, 2013, Houy, 2014]). Such an attack can occur when a miner can solve too many blocks in a row in expectation. It is usually said that this is the case when a miner owns strictly more than 50% of the hash power.[13] In order to make such an attack costly, the total hash rate of the Bitcoin network should be as large as possible. Since we did not consider the hash rate

[13]Actually, as we showed, at the outcome of the Bitcoin mining game, the probability to solve a block is not necessarily equal to the relative hash power.

A	B	C	D	E	F	G
GHash.IO	26.012%	0.40643	4648	20.682%	0.41929	3.164%
BTCGuild	22.736%	0.35525	3789	18.705%	0.36314	2.220%
Eligius	19.075%	0.29805	2911	16.303%	0.30219	1.389%
DiscusFish	11.946%	0.18666	1410	10.997%	0.18734	0.363%
Deepbit	9.056%	0.14150	869	8.591%	0.14170	0.144%
BitMinter	3.276%	0.05118	0	3.276%	0.05118	0.000%
Slush	3.083%	0.04817	0	3.083%	0.04817	0.000%
Bitparking	0.963%	0.01505	0	0.963%	0.01505	0.000%
BTCMine	0.963%	0.01505	0	0.963%	0.01505	0.000%
50BTC	0.963%	0.01505	0	0.963%	0.01505	0.000%
OzCoin	0.771%	0.01204	0	0.771%	0.01204	0.000%
Polmine	0.385%	0.00602	0	0.385%	0.00602	0.000%
P2Pool	0.385%	0.00602	0	0.385%	0.00602	0.000%
EclipseMC	0.193%	0.00301	0	0.193%	0.00301	0.000%
ASICMiner	0.193%	0.00301	0	0.193%	0.00301	0.000%

Table 4: With $R = 1.5625$ BTC, A: miner's name, B: relative hash power, C: expected reward when $\forall i \in N, x_i = 0$, D: optimal number of transaction included by miner i in the current block when $\forall j \in N \setminus \{i\}, x_j = 0$, E: probability to be the first miner to find a block reaching consensus when $\forall j \in N \setminus \{i\}, x_j = 0$ and x_i given in D, F: expected reward when $\forall j \in N \setminus \{i\}, x_j = 0$ and x_i given in D, G: (F-C) in %.

as an endogenous variable, what matters in our study when an agent makes his decision regarding the number of transactions to be included in his block is the ratio between the fixed and the variable rewards (R/c). However, the miners' benefits that will drive the hash rate purchase and hence eventually decide on the security of Bitcoin will depend on R and c in absolute values. This aspect has already been studied, though in a different context in [Houy, 2014b].

The second limitation is about the value of the Bitcoin network. Miners are rewarded in bitcoins. Hence, they have a vested interest in it to function well. And miners know that not processing transactions in their blocks means that Bitcoin loses some of its value as a mean of exchange. Hence, any reward they may earn from their mining activity has no value in this case. This suggests that the Bitcoin mining game should include a supplementary public good game.

Today, there is a debate in the Bitcoin developers community about the variable cost c. Should it be encoded and imposed in the protocol as it is partially today or should it be left to the market to decide its value? In the market case, if Bitcoin users want their transactions to be processed, then, they should attach to them a high enough fee. We believe that this paper gives a first result in the study of such a market: if a market was to be organized, with today's parameter, the transaction processing offer would be non null for transactions fees at least 0.0012BTC. We are rather uncertain about the relevance of

such a market because of the large externalities induced by the mining activity, some that we showed in this article, some that we showed in [Houy, 2014b].

References

[Andresen, 2013] Andresen G. (2013) "Back-of-the-envelope calculations for marginal cost of transactions", https://gist.github.com/gavinandresen/5044482. Retrieved on 03/03/2014.

[Decker and Wattenhofer, 2013] Decker C. and Wattenhofer R. (2013) "Information propagation in the Bitcoin network", 13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, September 2013.

[Eyal and Sirer, 2013] Eyal I. and Sirer E.G. (2013) "Majority is not enough: Bitcoin mining is vulnerable", arXiv: 1311.0243.

[Houy, 2014] Houy N. (2014) "It will cost you nothing to 'kill' a proof-of-stake crypto-currency", Working paper GATE 2014-04.

[Houy, 2014b] Houy N. (2014) "The economics of Bitcoin transaction fees", Working paper GATE 2014-07.

[Kroll *et al.*, 2013] Kroll J.A., Davey I.C. and Felten E.W. (2013) "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries", *Mimeo.*

[Krugman, 2013] Krugman P. (2013) "Adam Smith hates Bitcoin". NYTimes blog. http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/

[Nakamoto, 2008] Nakamoto S. (2009) "Bitcoin: a peer-to-peer electronic cash system".

Most of our analytical results are proved using the following lemmas.

Lemma 2 states that $\forall i \in N = \{1,2\}, \Pi_i(x_1,x_2)$ is continuous and has a continuous derivative with respect to x_i at $x_i = x_{3-i} > 0$.

Lemma 2

$\Pi^+(x_i,x_{3-i}) = \Pi^-(x_i,x_{3-i})$ *at* $x_i = x_{3-i}$.

Proof. With simple calculation, it is straightforward to show that $\Pi^+(x_i,x_{3-i}) = (R+cx_i)\alpha_i = \Pi^-(x_i,x_{3-i})$ in $x_i = x_{3-i}$. □

Lemma 3

$\dfrac{\partial \Pi^+(x_i,x_{3-i})}{\partial x_i} = \dfrac{\partial \Pi^-(x_i,x_{3-i})}{\partial x_i}$ *at* $x_i = x_{3-i}$.

Proof. It is easy to get

$$\frac{\partial \ln(\Pi^+(x_i,x_{3-i}))}{\partial x_i} = \frac{c}{R+cx_i} - \alpha_{3-i}\lambda k,$$

and

$$\frac{\partial \ln(\Pi^-(x_i,x_{3-i}))}{\partial x_i} = \frac{c}{R+cx_i} - \frac{\alpha_{3-i}\alpha_i k\lambda \exp\left(-\alpha_i\lambda(k(x_{3-i})-k(x_i))\right)}{\left(1-\alpha_{3-i}\exp\left(-\alpha_i\lambda(k(x_{3-i})-k(x_i))\right)\right)},$$

and it is straightforward to check that both are equal when $x_{-i} = x_i$. □

Lemma 4

$\dfrac{\partial^2 \Pi^-(x_i,x_{-i})}{\partial x_i^2} \geq 0$. *Moreover, if* $R > 0$ *or* $c > 0$, $\dfrac{\partial^2 \Pi^-(x_i,x_{-i})}{\partial x_i^2} < 0$.

Proof. Let $P(x_i,x_{-i}) = \alpha_{3-i}\exp\left(-\alpha_i\lambda(k(x_{3-i})-k(x_i))\right)$.

$$\Pi^-(x_i,x_{3-i}) = (R+cx_i)(1-P(x_i,x_{3-i})).$$

$$\frac{\partial \Pi^-(x_i,x_{3-i})}{\partial x_i} = c(1-P(x_i,x_{3-i})) - (R+cx_i)\alpha_i k\lambda P(x_i,x_{3-i})$$

$$\frac{\partial^2 \Pi^-(x_i,x_{3-i})}{\partial x_i^2} = -c\alpha_i\lambda k P(x_i,x_{3-i}) - c\alpha_i\lambda k P(x_i,x_{3-i}) - (R+cx_i)(\alpha_i\lambda k)^2 P(x_i,x_{3-i}) \leq 0.$$

Moreover, $\dfrac{\partial^2 \Pi^-(x_i,x_{3-i})}{\partial x_i^2} < 0$ if $R > 0$ or $c > 0$. □

Lemma 5

Assume $c > 0$. $\dfrac{\partial^2 \Pi^+(x_i,x_{-i})}{\partial x_i^2} < 0$ *whenever* $x_i < \dfrac{2}{\alpha_{3-i}\lambda k} - \dfrac{R}{c}$. *When* $x_i \geq \dfrac{2}{\alpha_{3-i}\lambda k} - \dfrac{R}{c}$, $\dfrac{\partial \Pi^+(x_i,x_{-i})}{\partial x_i} < 0$.

Assume $c = 0$ *and* $R > 0$. $\dfrac{\partial \Pi^+(x_i,x_{-i})}{\partial x_i} < 0$.

Proof. Let $P(x_i, x_{3-i}) = \alpha_i \exp\left(-\alpha_{3-i}\lambda(k(x_i) - k(x_{3-i}))\right)$.

$$\Pi^+(x_i, x_{3-i}) = (R + cx_i)P(x_i, x_{3-i}).$$

I. Assume $c > 0$.

$$\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i} = cP(x_i, x_{3-i}) - (R + cx_i)\alpha_{3-i}\lambda k P(x_i, x_{3-i}),$$

$$\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i} = cP(x_i, x_{3-i}) - (R + cx_i)\alpha_{3-i}\lambda k P(x_i, x_{3-i}),$$

$$\frac{\partial^2 \Pi^+(x_i, x_{-i})}{\partial x_i^2} = \alpha_{-i}\lambda k P(x_i, x_{-i})((R + cx_i)\alpha_{-i}\lambda k - 2c).$$

Then, obviously, $\frac{\partial^2 \Pi^+(x_i, x_{-i})}{\partial x_i^2} < 0$ whenever $x_i < \frac{2}{\alpha_{3-i}\lambda k} - \frac{R}{c}$. Then, obviously, $\frac{\partial^2 \Pi^+(x_i, x_{-i})}{\partial x_i^2} \geq 0$ whenever $x_i \geq \frac{2}{\alpha_{3-i}\lambda k} - \frac{R}{c}$.

$$\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i} = -cP(x_i, x_{3-i}) < 0$$

at $x_i = \frac{2}{\alpha_{3-i}\lambda k} - \frac{R}{c}$. Moreover, it is straightforward to check that $\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i}$ is negative when x_i is arbitrarily large. Then, necessarily, $\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i} < 0$ whenever $x_i \geq \frac{2}{\alpha_{3-i}\lambda k} - \frac{R}{c}$.

II. Assume $c = 0$.

$$\frac{\partial \Pi^+(x_i, x_{3-i})}{\partial x_i} = -R\alpha_{3-i}\lambda k P(x_i, x_{3-i}) < 0.$$

□

A Proof of Proposition 2

It is straightforward to check that $\frac{\partial \Pi^+(x_i, x^*_{3-i})}{\partial x_i} < 0$ and $\frac{\partial \Pi^-(x_i, x^*_{3-i})}{\partial x_1} < 0$ for on $\mathbb{R}^+$. Hence, by Lemma 2, $NE = \{(0, 0)\}$.

B Proof of Proposition 3

Assume $NE \neq \emptyset$. With no loss of generality, let us assume $x_1^* \geq x_2^*$. Then, $\Pi_1(x_1^*, x_2^*) = \Pi^+(x_1^*, x_2^*) = (R + c.x_1^*)\alpha_1 \exp\left(-\alpha_2\lambda(k(x_1^*) - k(x_2^*))\right)$. $\frac{\partial \Pi_1(x_1, x_2^*)}{\partial x_1} = \alpha_1 \exp\left(-\alpha_2\lambda(k(x_1) - k(x_2^*))\right)(c-$

$\alpha_2\lambda k(R+c.x_1))$ in $x_1 = x_1^*$ which has the sign of $(c-\alpha_2\lambda k(R+c.x_1^*))$. Then, by continuity of Π^+ and Lemmas 2, 3 and 5, we necessarily have $x_1^* = \max\{0, \frac{2}{\lambda k} - \frac{R}{c}\}$ or $x_1^* < x_2^*$ which contradicts the assumption that $x_1^* \geq x_2^*$.

Assume $0 > \frac{2}{\lambda k} - \frac{R}{c}$, then $x_1^* = 0$. By assumption, $x_2^* = 0$. Then, $\Pi_1(x_1^*, 0) = \Pi_1^+(x_1^*, 0)$ and it is straightforward to check that $\frac{\partial \Pi^+(x_1,0)}{\partial x_1} < 0$ at x_1^*. By Lemma 5, $x_1^* = 0$ is the only maximum of $\Pi^+(x_1, 0)$. Then, $NE = \{(0,0)\}$.

Assume $0 \leq \frac{2}{\lambda k} - \frac{R}{c}$. $x_1^* = \frac{2}{\lambda k} - \frac{R}{c}$. Now, it is straightforward to check that $\frac{\partial \Pi_2(x_1^*, x_2)}{\partial x_2} = \frac{\partial \Pi^-(x_2, x_1^*)}{\partial x_2} = 0$ in $x_2 = x_1^*$. By Lemmas 2, 3 and 4, $\arg\max_{x_2 \in \mathbb{R}^+} \Pi_2(x_1^*, x_2) = \frac{2}{\lambda k} - \frac{R}{c}$ and then, $NE = \{(\frac{2}{\lambda k} - \frac{R}{c}, \frac{2}{\lambda k} - \frac{R}{c})\}$.

Similarly to what has been shown above, it is straightforward to check that $(\frac{2}{\lambda k} - \frac{R}{c}, \frac{2}{\lambda k} - \frac{R}{c}) \in NE$ and then $NE \neq \emptyset$.

C Proof of Proposition 4

computing the mining mathematical problem with more transactions included in it is not more expensive in terms of CPU, disk or bandwidth. However, it should be considered that the larger a block, the longer it takes for it to be spread in the Bitcoin network and reach consensus. Then, including transactions in a block can have the adverse effect of lowering the probability of a miner to earn any reward. As we will show, this trade-off depends on how many transactions other miners include in their blocks themselves. Then, the number of transactions included in blocks is the outcome of a game: the Bitcoin mining game that we propose to study in this article.

Let $\alpha_1 > \alpha_2$ and assume that $NE \neq \emptyset$.

I. Assume $x_1^* \geq x_2^*$. Then, $\Pi_1(x_1^*, x_2^*) = \Pi^+(x_1^*, x_2^*) = (R+c.x_1^*)\alpha_1 \exp(-\alpha_2\lambda(k(x_1^*) - k(x_2^*)))$. $\frac{\partial \Pi_1(x_1, x_2^*)}{\partial x_1} = \alpha_1 \exp(-\alpha_2\lambda(k(x_1) - k(x_2^*)))(c-\alpha_2\lambda k(R+c.x_1))$ which has the sign of $(c-\alpha_2\lambda k(R+c.x_1))$. Then, by Lemmas 2, 3 and 4, we necessarily have $x_1^* = \max\{0, \frac{1}{\lambda k\alpha_2} - \frac{R}{c}\}$ or $x_1^* < x_2^*$ which contradicts the assumption that $x_1^* \geq x_2^*$.

a) Assume $\frac{1}{\lambda k\alpha_2} - \frac{R}{c} \geq 0$. Let us compute $\frac{\partial \Pi_2(x_1^*, x_2)}{\partial x_2}$ in $x_2 = x_1^*$. After simple computation, it has the sign of $c(1 - \frac{\alpha_1}{\alpha_2})$ and then is, since $\alpha_1 > \alpha_2$, strictly negative. By Lemmas 2, 3 and 4, this implies that the best response of miner 2 is unique and strictly below x_1^* if $x_1^* > 0$ or equal to x_1^* if $x_1 = 0$.

b) Assume $\frac{1}{\lambda k\alpha_2} - \frac{R}{c} < 0$ and hence $x_1^* = 0$. $\frac{\partial \Pi_2(x_1^*, x_2)}{\partial x_2}$ in $x_2 = x_1^*$ has the sign of

$c - \alpha_1 \lambda k R$. $\frac{1}{\lambda k \alpha_2} - \frac{R}{c} < 0$ and $\alpha_1 > \alpha_2$ imply $c - \alpha_1 \lambda k R < 0$.Then, $x_1^* = 0$ and $x_2^* = 0$ is the only Nash Equilibrium by Lemmas 2, 3 and 4.

II. Assume $x_2^* > x_1^*$. Then, $\Pi_2(x_1^*, x_2^*) = \Pi^+(x_2^*, x_1^*) = (R+c.x_2^*)\alpha_2 \exp\left(-\alpha_1 \lambda (k(x_2^*) - k(x_1^*))\right)$. $\frac{\partial \Pi_2(x_1^*, x_2)}{\partial x_2} = \alpha_2 \exp\left(-\alpha_1 \lambda (k(x_2) - k(x_1^*))\right)(c - \alpha_1 \lambda k (R+c.x_2))$ which has the sign of $(c - \alpha_1 \lambda k (R+c.x_2^*))$. Then, by Lemmas 2, 3 and 4, we necessarily have $x_2^* = \max\{0, \frac{1}{\lambda k \alpha_1} - \frac{R}{c}\}$ or $x_2^* < x_1^*$ which contradicts the assumption that $x_2^* > x_1^*$. Assume $x_2^* = 0$, this contradicts the assumption that $x_2^* > x_1^*$. Assume $x_2^* = \frac{1}{\lambda k \alpha_1} - \frac{R}{c} > 0$. Let us compute $\frac{\partial \Pi_1(x_1, x_2^*)}{\partial x_1}$ in $x_1 = x_2^*$. After simple computation, it has the sign of $c(1 - \frac{\alpha_2}{\alpha_1})$ and then is, since $\alpha_1 > \alpha_2$, strictly positive. By Lemmas 2, 3 and 4, this contradicts the fact that $x_2^* > x_1^*$.

Similarly to what has been shown above, it is straightforward to check that $NE \neq \emptyset$.